การพัฒนาระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect

ปิติ สุวรรณาคม[1*] และ อุทาน บูรณศักดิ์ศรี[1]

[1]คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ
*164480322004-st@rmutsb.ac.th

บทคัดย่อ

เนื่องจากปัจจุบันได้มีระบบแอปพลิเคชันเกิดขึ้นจำนวนมาก และไม่สามารถพัฒนาพร้อมกันได้ หรือถูกพัฒนาโดยหลายผู้ให้บริการ ผู้ใช้งานจึงต้องจดจำดิจิทัลไอดีเพื่อใช้บริการแต่ละเว็บแอปพลิเคชัน ส่งผลให้เกิดปัญหาในการลืมรหัสผู้ใช้หรือรหัสผ่านเพื่อเข้าใช้งาน แแม้ว่ามีการพัฒนาโพรโตคอลเข้าสู่ระบบเดียว (Single Sign On) เพื่อให้สามารถเข้าใช้งานได้หลายแอปพลิเคชันด้วยไอดีเดียวกัน แต่ผู้ใช้งานยังคงต้องจดจำรหัสผ่าน ดังนั้น งานวิจัยนี้มีวัตถุประสงค์เพื่อออกแบบและพัฒนาระบบการพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect เพื่อเพิ่มความปลอดภัยและความสะดวกในการเข้าถึงระบบสารสนเทศ นอกจากนี้ยังมีวัตถุประสงค์ในการศึกษาผลการใช้งานระบบ เพื่อประเมินประสิทธิภาพและผลกระทบของระบบใหม่ในการเข้าถึงระบบสารสนเทศ งานวิจัยนี้เสนอวิธีการแก้ปัญหาในการลืมรหัสผ่านและเพิ่มความปลอดภัยในการยืนยันตัวตน เพื่อเข้าถึงหลายแอปพลิเคชันด้วยไอดีเดียวกัน โดยใช้กุญแจส่วนตัวและเซ็นข้อมูลการยืนยันตัวตนด้วยรหัสภาพคิวอาร์โค้ดผ่านแอปพลิเคชันมือถือ งานวิจัยนี้สามารถยกระดับความน่าเชื่อถือของการยืนยันตัวตนไปถึงระดับ AAL ที่ระดับ 3 และเพิ่มความสะดวกให้กับผู้ใช้งาน นอกจากนี้ยังเป็นการพัฒนาต่อยอดจากโพรโตคอล OpenID Connect ซึ่งเป็นมาตรฐานในการเข้าถึงระบบสารสนเทศ

คำสำคัญ: การยืนยันตัวตน ไม่ใช้รหัสผ่าน โพรโตคอลเข้าสู่ระบบเดียว

Development of Password-less authentication on the OpenID Connect Protocol

Piti Suwannakom [1*] and Utharn Buranasaksee[1]

[1]Science and Technology Rajamangala University of Technology Suvarnabhumi
*164480322004-st@rmutsb.ac

Abstract

Due to the increasing number of applications being developed simultaneously or by multiple service providers, users are required to remember digital IDs for each web application, resulting in the problem of forgetting usernames or passwords. Although the Single Sign-On protocol, such as OpenID Connect, allows users to access multiple applications with a single ID, users still need to remember passwords. Therefore, this research aims to design and develop an authentication system without using passwords on the OpenID Connect protocol to enhance security and convenience in accessing information systems. Additionally, the study aims to evaluate the system's usability, effectiveness, and its impact on accessing information systems. This research proposes a solution to the problem of password forgetfulness and enhances security in identity verification by using private keys and QR code-based data signing through a mobile application. The research achieves an AAL level 3 in enhancing the credibility of identity verification and improves convenience for users. Furthermore, this work extends the capabilities of the OpenID Connect protocol, which is a standard for accessing information systems.

Keywords: Authentication, Password-less, Single Sign-on Protocol

1. บทนำ

เนื่องจากปัจจุบันได้มีระบบแอปพลิเคชันเกิดขึ้นจำนวนมาก โดยทั่วไประบบแอปพลิเคชันเหล่านี้ถูกพัฒนาไม่พร้อมกัน หรือถูกพัฒนาจากหลายผู้ให้บริการ ทำให้ผู้ใช้งานจะต้องจดจำดิจิทัลไอดีสำหรับใช้บริการเว็บแอปพลิเคนชันนั้น ดิจิทัลไอดีเป็นชุดข้อมูลที่ทำให้ผู้ใช้บริการสามารถยืนยันตัวตนกับผู้ให้บริการได้ โดยพื้นฐานดิจิทัลไอดีประกอบด้วยรหัสผู้ใช้และรหัสผ่าน การที่ผู้ใช้บริการมีบัญชีดิจิทัลไอดีจำนวนมากทำให้เกิดปัญหาลืมรหัสผู้ใช้หรือรหัสผ่านเพื่อเข้าใช้งาน อย่างไรก็ตามการยืนยันตัวตนด้วยรหัสผู้ใช้และรหัสผ่านยังมีความเสี่ยง เช่น การรั่วไหลของรหัสผ่าน แม้ว่าจะมีการยืนยันตัวตนแบบ 2 ปัจจัย ซึ่งใช้รหัสผ่านแบบ OTP ผ่านช่องทาง SMS หรือช่องทางอีเมลเพื่อช่วยบรรเทาปัญหาความมั่นคงปลอดภัย แต่วิธีการดังกล่าวมีความยุ่งยากในการใช้งาน เนื่องจากมีต้นทุนในการใช้งานที่สูง และผู้ใช้งานจะยังคงต้องจด จำรหัสผู้ใช้และรหัสผ่านเช่นเดิม ด้วยเหตุนี้ จึงมีการพัฒนาโพรโตคอลเข้าสู่ระบบเดียว (Single Sign On: SSO) [1] ที่ให้ผู้ใช้งานใช้ดิจิทัลไอดีเพียงบัญชีเดียว เพื่อให้สามารถเข้าใช้บริการได้หลายแอปพลิเคชัน เช่น OAuth 2.0 [2] หรือ Open ID Connect 1.0 [3] หรือ SAML 2.0 [4] ซึ่งโพรโตคอลเหล่านี้เป็นเพียงแค่การให้สิทธิ์การยืนยันตัวตนในการเข้าใช้บริการต่าง ๆ จากบัญชีดิจิทัลจากที่อื่นได้ แม้จะช่วยบรรเทาปัญหาการจดจำรหัสผู้ใช้และรหัสผ่านจำนวนมาก แต่การยืนยันตัวตนของผู้ใช้บริการทำให้ผู้ใช้บริการจำเป็นต้องจดจำรหัสผู้ใช้และรหัสผ่าน และปัจจัยการยืนยันตัวตนอื่นร่วมด้วยหากมีบังคับระดับความเข้มงวดในการยืนยันตัวตน นอกจากนี้ ในปัจจุบัน มีผู้ให้บริการหลายรายที่ให้บริการการยืนยันตัวตนผ่านโพรโตคอลเข้าสู่ระบบเดียว ทำให้ผู้ใช้งานมีแนวโน้มที่จะมีบัญชีดิจิทัลไอดีที่ใช้งานหลายบัญชี และแต่ละบัญชีอาจเข้าใช้งานหลายเว็บแอปพลิเคชัน จากปัญหาดังกล่าวพบว่าผู้ใช้งานยังประสบปัญหาเรื่องการลืมรหัสผ่าน เช่นเดิม

ดังนั้นจึงมีแนวคิดคือพัฒนาการยืนยันตัวตนให้มีระดับที่สูงขึ้น เช่น การใช้กุญแจส่วนตัวมาเพื่อเข้าสู่ระบบ ประโยชน์ของการใช้กุญแจส่วนตัวคือการเพิ่มระดับของความปลอดภัยให้เป็นระดับสูงสุด ซึ่งในปัจจุบันก็ได้มีหลายระบบที่มีการยืนยันตัวตนด้วยกุญแจส่วนตัวอยู่แล้ว เช่น การที่ผู้ดูแลระบบจะเข้าเครื่องแม่ข่าย (SSH Protocol) [5] หรือการที่นักพัฒนาซอฟต์แวร์จะอัปโหลดซอร์สโค้ดเข้าไปยัง Git หรือการอัปโหลดซอร์สโค้ดก็จะมีผู้ให้บริการ เช่น Bitbucket [6], GitHub [7], GitLab [8] ซึ่งผู้ให้บริการนี้จะให้ใช้กุญแจส่วนตัวเป็นค่าเริ่มต้นในการยืนยันตัวตน โดยทั่วไปผู้เชี่ยวชาญทางด้านไอทีหรือนักพัฒนาซอฟต์แวร์จะใช้กุญแจส่วนตัวในการยืนยันตัวตน แต่กลุ่มคนผู้ใช้ทั่วไปยังไม่ได้ตระหนักถึงการใช้กุญแจส่วนตัวในการยืนยันตัวตนในระบบต่าง ๆ

ปัจจุบันรูปแบบการพิสูจน์ตัวตน ยังจะมีรูปแบบใหม่เป็นโพรโตคอลมาตรฐานที่จะใช้กุญแจส่วนตัวในการพิสูจน์ตัวตนโดยไม่ต้องใช้รหัสผ่าน เช่น WebAuthn [9] หรือ FIDO2 [10] จาก Fast Identity Online Alliance จากบริษัททางเทคโนโลยีชั้นแนวหน้าของโลก อย่างเช่น Apple, Google และ Microsoft ได้ร่วมกันพัฒนารูปแบบการลงชื่อเข้าใช้บริการโดยไม่ใช้รหัสผ่านสำหรับเว็บไซต์หรือแอปพลิเคชัน ซึ่งเป็นการเซ็นธุรกรรมโดยที่ไม่ต้องอัปโหลดกุญแจส่วนตัวขึ้นไปบนระบบ โดยใช้โปรแกรมเสริมของเบราว์เซอร์ทำการเลือกกุญแจส่วนตัว เพื่อทำการเซ็นธุรกรรมในการล็อกอินเข้าระบบ แต่จะมีปัญหาที่สามารถทำได้แค่บนเครื่องคอมพิวเตอร์หรือแลปท็อปเท่านั้น และถ้าใช้ในโทรศัพท์มือถือจะติดปัญหาในส่วนของเบราว์เซอร์ไม่สามารถติดตั้งโปรแกรมส่วนเสริมนั้นได้ หรือถ้าจำเป็นต้องการใช้งานจากเครื่องอื่นที่ไม่ใช่เครื่องส่วนตัว เช่น ที่ห้องสมุดสาธารณะ หรือในร้านอินเทอร์เน็ตคาเฟ่ต่าง ๆ จะมีปัญหาในการคัดลอกกุญแจส่วนตัวเพื่อใช้สำหรับการยืนยันตัวตน

จากงานวิจัยก่อนหน้า Jirapong Sae-tang & Wilawan Rukpakavong [11] ได้กล่าวถึงการผนวกตำแหน่งกับรหัสผ่านครั้งเดียวโดยเข้ารหัสแบบกุญแจสาธารณะสำหรับการพิสูจน์ตัวตน แต่งานวิจัยถูกนำไปใช้กับการพิสูจน์ตัวตนระหว่างเครื่องเอทีเอ็มกับแอปพิลเคชันบนโทรศัพท์ ซึ่งมีข้อจำกัดในการใช้งานเฉพาะกลุ่มที่เป็นแอปพลิเคชันของธนาคารเอง และการจะได้รับกุญแจส่วนตัวสำหรับการเข้ารหัสนั้นถูกสร้างจากเซิร์ฟเวอร์ของธนาคารก็มีจุดอ่อนตรงที่การจะส่งกุญแจส่วนตัวมายังแอปพลิเคชันบนโทรศัพท์มือถือซึ่งจะทำได้ยากและมีความเสี่ยง โดยปกติ การสร้างกุญแจส่วนตัวจะต้องสร้างที่ตัวแอปพลิเคชันบนโทรศัพท์เอง และจะไม่ถูกย้ายหรือส่งออกจากแอปพลิเคชันบนโทรศัพท์ สำหรับการเชื่อมต่อ งานวิจัยดังกล่าวไม่ได้ใช้โพรโตคอลมาตรฐาน เช่น OAuth หรือ OpenID Connect เพื่อเชื่อมต่อ ดังนั้นจึงเป็นการยากที่จะนำไปใช้กับแพลตฟอร์มอื่น หรือถ้าทำก็ต้องปรับเปลี่ยนกระบวนการยืนยันตัวตนที่ให้ผู้ใช้งานใช้รหัสดิจิทัลไอดีเพียงบัญชีเดียว

จากปัญหาดังกล่าว นักวิจัยได้มองเห็นปัญหานี้ ซึ่งนำมาสู่การพัฒนาระบบการพิสูจน์ตัวตนที่ใช้กุญแจส่วนตัวเพื่อตรวจสอบตัวตน โดยที่ผู้ใช้ไม่ต้องระบุรหัสผ่าน ดังนั้นผู้วิจัยจึงออกแบบโพรโตคอลที่มีฟังก์ชันการทำงานของระบบที่สามารถเข้าสู่ระบบด้วยกุญแจส่วนตัวได้ โดยมีเงื่อนไขว่าให้กุญแจส่วนตัวอยู่ในอุปกรณ์เครื่องนึง เช่น คอมพิวเตอร์ หรือโทรศัพท์มือถือ แต่อุปกรณ์ที่ต้องการเข้าสู่ระบบจะเป็นคอมพิวเตอร์หรือโทรศัพท์มือถือเครื่องอื่น โดยไม่ต้องติดตั้งโปรแกรมเสริมลงในเบราว์เซอร์ หรือต้องคัดลอกกุญแจส่วนตัวลงในอุปกรณ์ที่จะล็อกอิน ผู้วิจัยได้พัฒนาวิธีที่ทำให้เราสามารถเข้าสู่ระบบของโทรศัพท์มือถือได้อย่างง่ายดาย ซึ่งมีคุณสมบัติที่สำคัญคือการมีกล้องในโทรศัพท์มือถือ วิธีการที่เราใช้คือการสแกนรหัส QR และลบชุดรหัสที่ระบุโดยเซสชันของเบราว์เซอร์ จากนั้น เราจะส่งชุดรหัสนั้นไปยังแอปพลิเคชันมือถือและเซ็นรายการเพื่อบอกว่าเซสชันของเบราว์เซอร์จะถูกบันทึกในนามของเรา

2. วัตถุประสงค์

2.1 เพื่อออกแบบระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect

2.2 เพื่อพัฒนาระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect

2.3 เพื่อศึกษาผลการใช้งานระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect

3. วิธีการศึกษา

การศึกษาวิจัยเรื่องการพัฒนาระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect ผู้วิจัยดำเนินการวิจัยตามขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 ผู้วิจัยจะต้องศึกษาข้อมูลเอกสารงานวิจัยที่เกี่ยวข้อง และการเก็บรวบรวมข้อมูล เพื่อออกแบบระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect

ขั้นตอนที่ 2 ผู้วิจัยวิเคราะห์และออกแบบระบบเพื่อศึกษาความเป็นไปได้ในการพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect และมีความน่าเชื่อถือ ตลอดจนแก้ไขปัญหาดังที่ได้กล่าวมาได้

ขั้นตอนที่ 3 ผู้วิจัยดำเนินการพัฒนาระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect โดยใช้ภาษา PHP

ขั้นตอนที่ 4 เมื่อนำระบบไปติดตั้งและเชื่อมต่อกับแอปพลิเคชันจริงในแซนด์บ็อกซ์ (Sandbox) ผู้วิจัยประเมินผลการพัฒนาระบบเชิงคุณภาพโดยเปรียบเทียบคุณสมบัติของระบบที่พัฒนาขึ้นมากับวิธีการที่ในงานก่อนหน้าเพื่อเปรียบเทียบข้อดีข้อเสียวิธีการที่ผู้วิจัยได้นำเสนอ

4. ผลการศึกษาและอภิปรายผล

จากขั้นตอนการศึกษาผู้วิจัยได้ศึกษางานวิจัยและวรรณกรรมที่เกี่ยวข้องและรวบรวมข้อมูลปัญหาที่เกี่ยวข้องกับการยืนยันตัวตน เพื่อวิจัยศึกษาค้นคว้าและสร้างระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect โดยที่ การยืนยันตัวตนจะใช้ชุดกุญแจคู่ในการยืนยันตัวตน และไม่มีการเก็บกุญแจส่วนตัวไว้ที่ระบบ และเพื่อไม่ให้เกิดความยุ่งยากในการจัดเก็บและการใช้งานชุดกุญแจคู่ ผู้ใช้ไม่จำเป็นจะต้องสร้างหรือทำการคัดลอกชุดกุญแจคู่ติดตัวไปตลอด ผู้วิจัยจึงใช้แอปพลิเคชันในโทรศัพท์มือถือในการสร้างและจัดเก็บชุดกุญแจคู่ และใช้ทำการเซ็นธุรกรรมในการยืนยันตัวตน

การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key cryptography) เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัสทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

การเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัสคือ กุญแจสาธารณะ (public key) เป็นกุญแจที่ผู้สร้างสามารถเปิดเผยได้ และกุญแจส่วนตัว (private key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

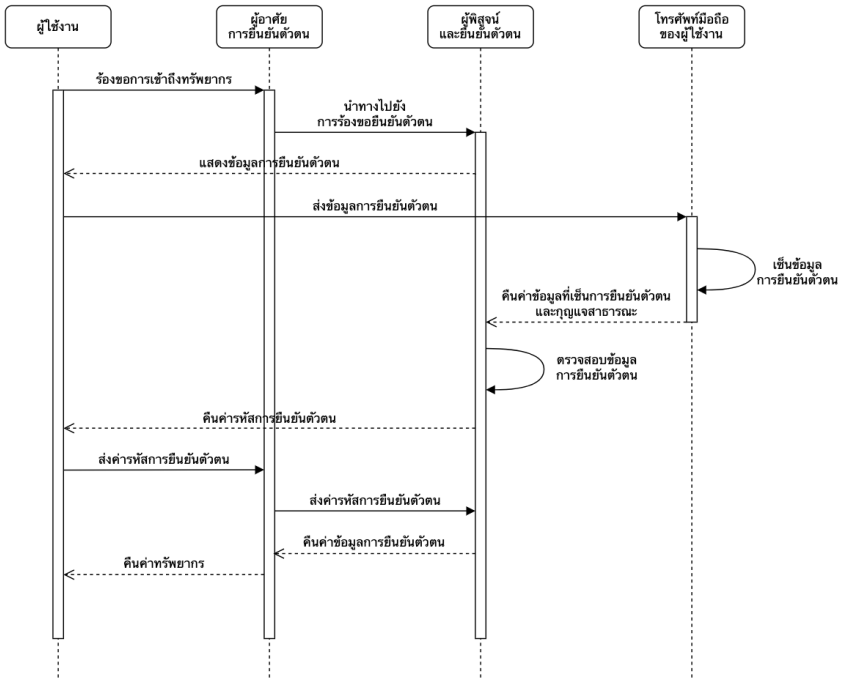
การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส (Encryption) และการพิสูจน์ตัวตน (Authentication) การประยุกต์ใช้ในการเข้ารหัสข้อมูลจะกระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ คือ 1) ผู้ใช้แต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้ารหัสและการถอดรหัส 2) กุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้คนอื่นๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง 3) เมื่อจะส่งข้อมูลออกไปหาผู้ใช้คนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะ ก่อนถูกส่งออกไป 4) เมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันในการถอดรหัสข้อมูลได้อย่างถูกต้อง

การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้ 1)เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชันทางคณิตศาสตร์ที่เรียกว่า "แฮชฟังก์ชัน" ได้เมสเซสไดเจสต์ (Message Digest) ออกมา 2) การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับ สามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้ 3) การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และถอดรหัสลายเซ็นอิเล็กทรอนิคส์ด้วยกุญแจสาธารณะของผู้ส่ง ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยันข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง

Oauth 2.0 เป็น Authorization Framework ของระบบยืนยันตัวตน (Authentication) และการจัดการสิทธิ์ (Authorization) เปิดให้ Third-Party Application (Client) ได้รับสิทธิ์การเข้าถึงการเข้าใช้งานระบบต่างๆ ตามข้อกำหนดของมาตรฐาน RFC6749 ที่ IETF : Internet Engineering Task Force กำหนดขึ้นมา ที่ให้สำหรับ Client เชื่อมต่อโดยใช้ Access Token แทนรหัสผู้ใช้งาน และรหัสผ่าน เพื่อนำไปใช้กับบริการอื่นๆ ทำให้มีความปลอดภัยมากขึ้น รวมไปถึงจัดการสิทธิ์ว่าสามารถทำอะไรได้บ้างกับบริการนั้นๆ ซึ่ง OAuth 2.0 จะใช้โพรโตคอลที่เรียกว่า “OpenID Connect” หรือ OIDC ดังนั้นเมื่อเราทำ Authentication โดยใช้ OAuth 2.0 นั่นแปลว่าเรากำลังใช้ OIDC อยู่

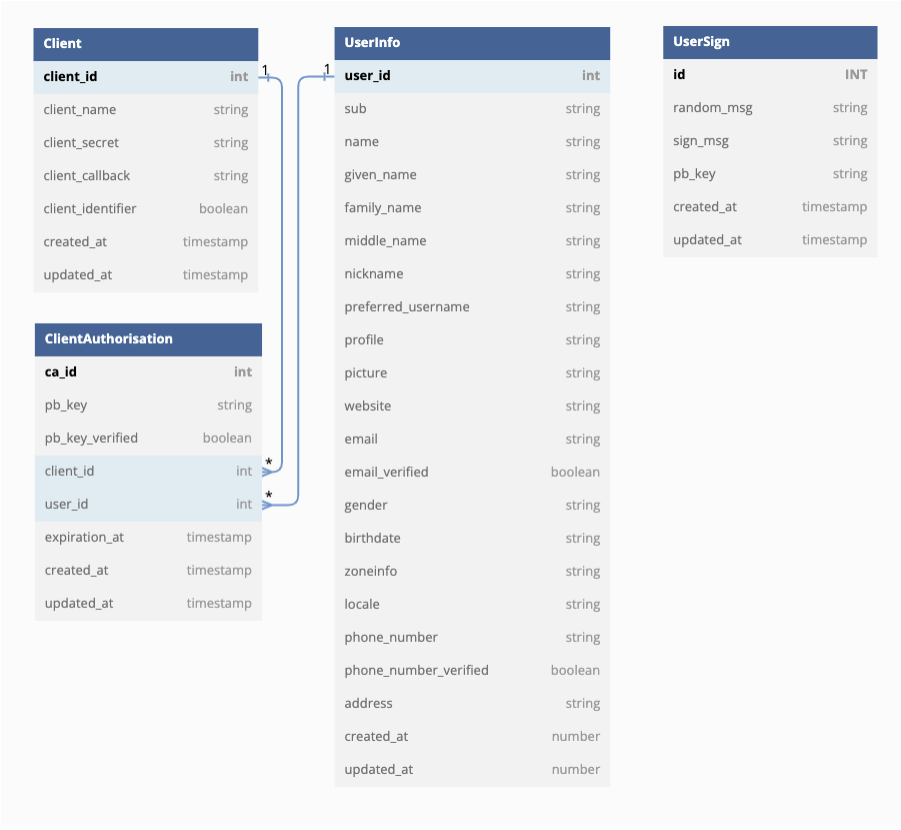
OpenID Connect เป็นโพรโตคอลพื้นฐานที่โพรโตคอล OAuth 2.0 ใช้งานอยู่ ซึ่งจะช่วยให้ไคลเอนต์สามารถตรวจสอบตัวตนของผู้ใช้ปลายทางตามการรับรองความถูกต้องที่ดำเนินการโดย Authorization Server ซึ่งจะประกอบไปด้วย Relying party (RP) ในที่นี้ทางผู้วิจัยจะเรียกว่า ผู้ให้บริการทรัพยากร และ Identity provide (idP) ในที่นี้ทางผู้วิจัยจะเรียกว่า ผู้ให้บริการการพิสูจน์ตัวตน

ต่อมาในขั้นตอนที่ 2 การออกแบบระบบผู้วิจัยวิเคราะห์และออกแบบระบบเพื่อศึกษาความเป็นไปได้ในการพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect โดยผู้วิจัยมุ่งเน้นเรื่องของกระบวนการยืนยันตัวตนด้วยชุดรหัสกุญแจคู่ ในการวิเคราะห์และออกแบบระบบ ดังภาพที่ 1 กระบวนการจึงเริ่มต้นจากการที่ผู้ใช้งานร้องขอการเข้าถึงทรัพยากร ผู้อาศัยการยืนยันตัวตนจะนำทางไปยังการร้องขอยืนยันตัวตน จากนั้นผู้พิสูจน์ตัวตนจะแสดงข้อมูลการยืนยันตัวตนด้วยรหัสภาพคิวอาร์โค้ด ผู้ใช้งานจะใช้แอปพลิเคชันมือถือสแกนรหัสภาพคิวอาร์โค้ดเพื่อทำการเซ็นข้อมูลการยืนยันตัวตน จากนั้นโทรศัพท์มือถือจะคืนค่าข้อมูลที่เซ็นการยืนยันตัวตน (Signature) และกุญแจสาธารณะ (Public Key) ไปยังผู้พิสูจน์และยืนยันตัวตนเพื่อตรวจสอบข้อมูล เมื่อตรวจสอบแล้วว่าถูกต้องจะคืนค่ารหัสการยืนยันตัวตน (Access Token) ไปยังผู้ใช้งาน แล้วผู้ใช้งานจะใช้ค่ารหัสการยืนยันตัวตน (Access Token) ในการเข้าใช้ระบบ เพื่อให้ผู้อาศัยการยืนยันตัวตนสามารถนำรหัสการยืนยันตัวตน (Access Token) ไปตรวจสอบกับผู้พิสูจน์และยืนยันตัวตนได้ ถึงจะเสร็จกระบวนการยืนยันตัวตน



ภาพที่ 1 Sequence diagram ของระบบ

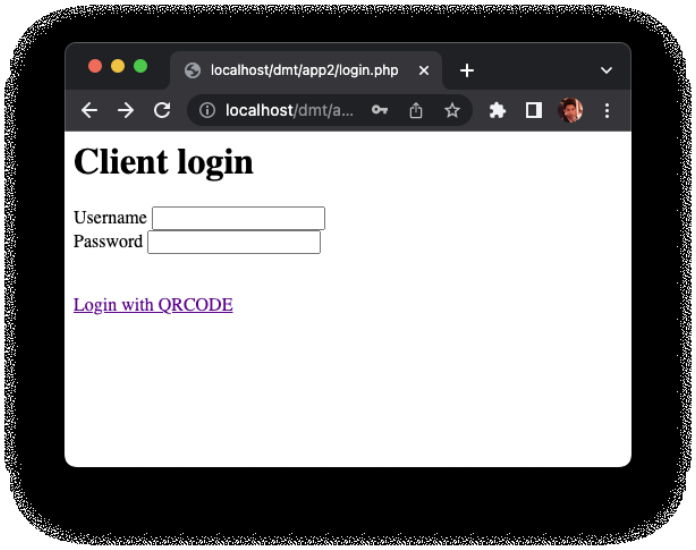
การออกแบบฐานข้อมูล ผู้วิจัยจะใช้มาตรฐานของ OpenID Connect 1.0 Standard Claims ในการออกแบบการบันทึกข้อมูลผู้ใช้งาน ดังภาพที่ 2 และการเก็บข้อมูลการยืนยันตัวตน ระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect นั้นจะเก็บเพียงแค่กุญแจสาธารณะที่เอาไว้ระบุตัวตนสำหรับการคืนค่าการยืนยันตัวตนของผู้ใช้งาน



ภาพที่ 2 สถาปัตยกรรมของระบบ

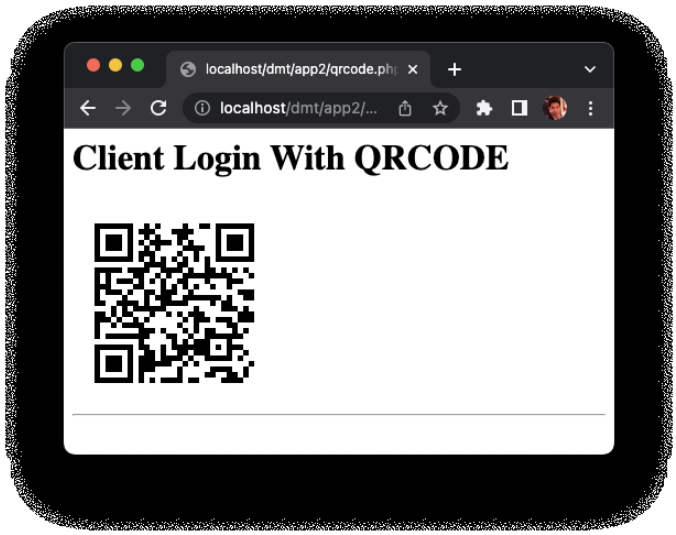
ขั้นตอนที่ 3 ผู้วิจัยดำเนินการพัฒนาระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่านบนโพรโตคอล OpenID Connect โดยใช้ภาษา PHP เป็นระบบยืนยันตัวตนโดยไม่ใช้รหัสผ่าน โดยการใช้การเซ็นธุรกรรมโดยใช้ชุดกุญแจคู่ผ่านแอปพลิเคชันมือถือ เมื่อผู้ใช้งานทำการล็อกอินระบบผ่านคอมพิวเตอร์ ระบบจะทำการสร้างชุดรหัสที่ระบุโดยเซสชันของเบราว์เซอร์ (Random Message) และที่อยู่ของเบราว์เซอร์ย้อนกลับ (Callback URL) มาสร้างรหัสภาพคิวอาร์โค้ดเพื่อผู้ใช้งานนำโทรศัพท์มือถือที่ทำการติดตั้งแอปพลิเคชันสำหรับการสแกนคิวอาร์โค้ดมาเซ็นข้อมูลการยืนยันตัวตน (Signature) และทำการส่งค่ากลับมายังระบบยืนยันตัวตนพร้อมกับกุญแจสาธารณะ (Public Key) เพื่อระบุตัวตนผู้ใช้ ส่วนกระบวนการพิสูจน์ตัวตนโดยการนำข้อมูลการยืนยันตัวตน (Signature) มาถอดรหัสด้วยกุญแจสาธารณะ (Public Key) หากถอดรหัสผ่าน ระบบจะสร้างค่ารหัสการยืนยันตัวตน (Access Token) จัดเก็บข้อมูลการยืนยันตัวตน จะทำการส่งข้อมูลผู้ใช้กลับไปยังระบบผ่านโพรโตคอล OpenID Connect เพื่อให้ผู้ใช้งานเข้าใช้งานระบบได้

ผู้วิจัยได้ทำการพัฒนาระบบโดยเริ่มจากการปรับหน้าจอล็อกอินเพื่อเข้าสู่ระบบโดยการเพิ่มช่องทางการล็อกอินด้วยคิวอาร์โค้ด ดังภาพที่ 3 เพื่อเข้าสู่กระบวนการยืนยันตัวตนผ่านโพรโตคอล OpenID Connect



ภาพที่ 3 ตัวอย่างหน้าจอล็อกอินเข้าสู่ระบบ

เมื่อทำการเลือกการล็อกอินเข้าสู่ระบบด้วยคิวอาร์โค้ดระบบจะแสดงผลตามภาพที่ 4 เพื่อให้ผู้ใช้งานใช้แอปพลิเคชันในโทรศัพท์มือถือทำการสแกนรหัสภาพคิวอาร์โค้ดเพื่อทำการยืนยันตัวตนเพื่อเข้าสู่ระบบ



ภาพที่ 4 ตัวอย่างหน้าจอล็อกอินเข้าสู่ระบบ

ขั้นตอนที่ 4 เมื่อนำระบบไปติดตั้งและเชื่อมต่อกับแอปพลิเคชันจริงในแซนด์บ็อกซ์ (Sandbox) ผู้วิจัยประเมินผลการพัฒนาระบบเชิงคุณภาพดัง ตารางที่ 1 แสดงการเปรียบเทียบคุณสมบัติของระบบที่พัฒนาขึ้นมากับวิธีการที่ในงานก่อนหน้าเพื่อเปรียบเทียบข้อดีข้อเสีย จะเห็นได้ว่าวิธีที่นำเสนอในงานวิจัยฉบับนี้สามารถทำการยืนยันตัวตนด้วยชุดกุญแจคู่ ทำให้มีความปลอดภัยการการยืนยันตัวตนสูง และผู้ใช้งานไม่ต้องจดจำรหัสผู้ใช้และรหัสผ่าน และไม่ต้องยุ่งยากในการคัดลอกชุดกุญแจคู่ไปยังคอมพิวเตอร์เครื่องอื่น ๆ ที่จะต้องการยืนยันตัวตน มีความสะดวกสบายต่อผู้ใช้ และมีความรวดเร็วในการทำธุรกรรม

ตารางที่ 1 เปรียบเทียบคุณสมบัติวิธีการที่นำเสนอ

คุณสมบัติ	**รหัสผู้ใช้และรหัสผ่าน**	**รหัสผู้ใช้และรหัสผ่าน และมีการยืนยัน OTP**	**ระบบพิสูจน์ตัวตนโดยไม่ใช้รหัสผ่าน**
ปัญหาการลืมรหัสผ่าน	ต้องจดจำรหัสผู้ใช้และรหัสผ่าน	ต้องจดจำรหัสผู้ใช้และรหัสผ่าน	ไม่ต้องใช้รหัสผ่าน
ความสะดวกสบายของผู้ใช้	ต้องระบุรหัสผู้ใช้และรหัสผ่าน	ต้องระบุรหัสผู้ใช้ รหัสผ่าน และต้องระบุรหัส OTP อีกครั้ง	ใช้โทรศัพท์มือถือในการสแกนรหัสภาพคิวอาร์โค้ด
ระดับ AAL	ระดับ 1	ระดับ 2	ระดับ 3
ค่าใช้จ่าย OTP	ไม่มีค่าใช้จ่าย	มีค่าใช้จ่าย	ไม่มีค่าใช้จ่าย
ความเร็วในการทำธุรกรรม	หากระบุรหัสผู้ใช้และรหัสผ่านถูกต้องสามารถเข้าใช้งานได้เลย	หากระบุรหัสผู้ใช้และรหัสผ่านถูกต้อง จะต้องรอรหัส OTP	ใช้โทรศัพท์มือถือในการสแกนรหัสภาพคิวอาร์โค้ดเสร็จแล้วสามารถเข้าใช้งานได้เลย

5. สรุปผล

จากปัญหาที่ผู้ใช้ส่วนใหญ่จะลืมรหัสผู้ใช้หรือรหัสผ่านในการเข้าใช้งาน งานวิจัยนี้ได้แก้ปัญหาโดยการยืนยันตัวตนโดยไม่ใช้รหัสผ่าน และปัญหาด้านความปลอดภัยในการที่ผู้ใช้งานมักจะมีความเสี่ยงในการที่จะถูกขโมยรหัสผ่าน การโดนฟิชชิ่ง การสุ่มรหัสผ่าน แม้ว่ามีการพัฒนาโพรโตคอลเข้าสู่ระบบเดียว (Single Sign On) เพื่อให้สามารถเข้าใช้บริการได้หลายแอปพลิเคชันโดยใช้ดิจิทัลไอดีเดียว แต่ผู้ใช้ยังคงต้องจดจำรหัสผ่าน งานวิจัยนี้ได้แก้ปัญหาโดยใช้หลักการเข้ารหัสโดยใช้กุญแจส่วนตัวเพื่อเซ็นข้อมูลการยืนยันตัวตน และยกระดับความน่าเชื่อถือของการยืนยันตัวตนให้เป็น AAL ที่ระดับ 3 และจากปัญหาที่ผู้ใช้ทั่วไปมีความยุ่งยากในการใช้งานกุญแจส่วนตัว งานวิจัยนี้ได้แก้ปัญหาโดยการใช้แอปพลิเคชันมือถือสร้างกุญแจส่วนตัวและทำการเซ็นข้อมูลการยืนยันตัวตนด้วยรหัสภาพคิวอาร์โค้ด ทำให้ผู้ใช้งานไม่ต้องทำการคัดลอกกุญแจส่วนตัวไปยังคอมพิวเตอร์เครื่องอื่น ๆ งานวิจัยนี้ต่อยอดจากโพรโตคอล OpenID Connect ซึ่งเป็นโพรโตคอลมาตรฐานทำให้สามารถใช้งานกับระบบสารสนเทศอื่นที่มีในปัจจุบัน

งานวิจัยต่อไปตรวจสอบเรื่องของความมั่นคงปลอดภัยของระบบที่พัฒนา เพื่อให้สามารถนำไปใช้ในระบบจริงได้อย่างปลอดภัย และตรวจหาและแก้ไขช่องโหว่ที่อาจเกิดขึ้นในการใช้งานจริง พร้อมศึกษาและเข้าใจปัญหาที่เกี่ยวข้องกับการใช้งานระบบสำหรับการยืนยันตัวตนที่มีความมั่นคงปลอดภัยและเป็น AAL ระดับ 3 และสร้างวิธีการแก้ไขปัญหาที่เกี่ยวข้องอย่างเหมาะสม

6. เอกสารอ้างอิง

[1] Fett, D. Küsters, R. & Schmitz, G. The web sso standard openid connect: In-depth formal security analysis and security guidelines. In: 2017 IEEE 30th computer security foundations symposium (CSF). IEEE; 2017, p. 189–202.

[2] Hardt, D. (2012). The OAuth 2.0 authorization framework. Retrieved 8 October 2022. https://www.rfc-editor.org/rfc/rfc6749.

[3] Sakimura, N., Bradley, J., Jones, M., De Medeiros, B. & Mortimore, C. (2014). OpenID connect core 1.0 incorporating errata set 1. Retrieved 8 October 2022. https://openid.net/specs/openid-connect-core-1_0.html.

[4] Microsoft. (2022). Single sign-on SAML protocol. Retrieved 8 October 2022. https://docs.microsoft.com/en-us/azure/active-directory/develop/single-sign-on-saml-protocol.

[5] T. Ylonen & C. Lonvick. The secure shell (SSH) protocol architecture. RFC 4251. Jan. 2006.

[6] Atlassian Inc. (2023). Set up an SSH key. Retrieved 8 October 2022. https://support.atlassian.com/bitbucket-cloud/docs/set-up-an-ssh-key.

[7] GitHub Inc. (2023). Connecting to GitHub with SSH. Retrieved 8 October 2022. https://docs.github.com/en/authentication/connecting-to-github-with-ssh.

[8] GitLab Inc. (2023). Use SSH keys to communicate with GitLab. Retrieved 8 October 2022. https://docs.gitlab.com/ee/user/ssh.html.

[9] Suby Raman. (2023). WebAuthn. Retrieved 8 October 2022. https://webauthn.guide.

[10] FIDO2 Alliance. (2023). FIDO2: WebAuthn & CTAP. Retrieved 8 October 2022. https://fidoalliance.org/fido2.

[11] Sae-tang, J. & Rukpakavong, W. (2020). King Mongkut's University of Technology North Bangkok. National Conference on Computing and Information Technology (NCCIT 2020). Combining location with one time password by using public key encryption for authentication.